前　言

GB 17859—1999《计算机信息系统安全保护等级划分准则》是我国计算机信息系统信息安全等级管理的重要标准，已于 1999 年 9 月 13 日发布。为促进计算机信息系统安全等级管理工作正常有序地开展，特制定一系列相关的标准，包括：

——计算机信息系统安全等级保护技术要求系列标准；

——计算机信息系统安全等级保护评估准则系列标准；

——计算机信息系统安全等级保护工程管理要求；

——计算机信息系统安全等级保护管理要求。

本标准为以上相关系列标准之一。

本标准的附录 A 中列出了等级要求对照表。

本标准的附录 A 是资料性附录。

本标准由公安部公共信息网络安全监察局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部公共信息网络安全监察局、中国电子科技集团第三十研究所、上海三零卫士信息安全有限公司。

本标准主要起草人：张建军、魏忠、叶铭、陈克军、卿昊、吴晓星。

引　言

本标准所指的信息系统安全等级保护工程是指按照 GB 17859—1999 及其相关配套标准对计算机信息系统安全等级管理的要求，对信息网络系统、信息应用系统和信息资源开发等项目的新建、扩建和升级。

本标准不仅是计算机信息系统安全等级保护工程实施的指南，而且也是实施计算机信息系统安全等级保护工程、建立工程实施保证体系的依据，同时也是国家相应主管部门进行计算机信息系统安全工程等级评审的依据。本标准可作为甲方、乙方、第三方进行安全保护工程建设时的参考，也可作为制定与安全保护工程质量相关的法令、法规、标准的依据和参考。

计算机信息系统安全等级保护
工程管理要求

1 范围

本标准规定了计算机信息系统安全工程(以下简称信息安全工程)管理的要求,是对信息安全工程中所涉及到的甲方、乙方与第三方实施安全工程的指导性文件,各方可以此为依据建立安全项目的安全工程管理体系。

本标准按照 GB 17859—1999 划分的五个安全保护等级,规定了对不同安全保护等级的计算机信息系统进行工程实施采用不同安全要求。

本标准按照 GB 17859—1999 的五个安全保护等级的要求,适用于有关信息安全的计算机信息系统开发与集成工程管理,对于提供安全服务和安全工程组织的机构也可参照使用。

本标准适用于安全系统的机构和开发商的工程管理,集成商、安全服务的提供商和安全工程的组织商也可参照使用。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB 17859—1999 计算机信息系统安全保护等级划分准则

GA/T 390—2002 计算机信息系统安全等级保护通用技术要求

GA/T 391—2002 计算机信息系统安全等级保护管理要求

3 术语和定义

下列术语和定义适用于本标准。

3.1

信息安全 information security

信息的保密性、完整性和可用性。

3.2

甲方 owner

信息系统安全工程的投资者(或拥有人),代表信息系统安全工程建设的需求方。

3.3

乙方 developer

承担信息系统安全工程建设的实体,通过自身的努力,建设信息系统安全工程,满足信息系统建设者的安全需求。

3.4

第三方 third party

独立于甲、乙两方的组织或机构。

3.5

安全工程 security engineering

为了确保信息系统的保密性、完整性、可用性等目标而进行的系统工程活动。

3.6

安全工程相关的活动　security engineering related activity

与安全工程相关的其他工程活动，其中包括：企业工程、系统工程、软件工程、人力工程、通信工程、硬件工程、测试工程和系统管理。

3.7

安全工程的生命期　security engineering lifecycle

在整个信息系统生命期中执行的安全工程活动包括：概念形成、概念开发和定义、验证与确认、工程实施开发与制造、生产与部署、运行与支持和终止。

3.8

组织　organization

按一定宗旨和系统建立起来的集体。

3.9

项目　project

项目是各种相关实施活动和资源的总和，这些实施活动和资源用于开发或维护信息安全工程。一个项目往往有相关的资金，成本账目和交付时间表。

3.10

过程　process

将一个或多个输入进行一系列结构化处理，并将处理结果转化为对用户有价值的相互关联或相互作用的活动。

3.11

脆弱性　vulnerability

系统中存在的弱点，安全漏洞，或实施缺陷等非设计意图的部分，可被威胁利用对系统进行攻击。

3.12

过程能力　process capability

评估组织遵循工程过程能力的量化指标。

3.13

过程成熟度　process maturity

表明一个特定过程被清晰定义、管理、测量、控制的程度和有效性。

3.14

过程管理　process management

一系列用于预见、评价和控制过程执行的活动和体系结构。

3.15

安全工程指南　security engineering guide

由工程组做出的有关如何选择工程体系结构、设计与实现的决定。

3.16

关键资源　key resource

对项目成功与否有决定性影响的重要资源。

4　安全工程体系

4.1　概述

计算机信息系统安全工程等级保护要求体系结构可在整个安全工程范围内决定安全工程的要求等级。本标准使用这个体系结构的目标是清晰地从管理和制度化特征中分离出安全工程的基本特征，建

立安全工程的等级管理模型。

4.2 安全工程目标

理解用户的安全风险，根据已识别的安全风险建立合理的安全要求，将安全要求转换成安全指南，这些安全指南指导项目实施的其他活动，在正确有效的安全机制下建立对信息安全的信心和保证；判断系统中和系统运行时残留的安全脆弱性，及其对运行的影响是否可容忍(即可接受的风险)，使安全工程成为一个可信的工程活动，能够满足相应等级信息系统设计的要求。

4.3 基本模型

由安全等级、保障与实施组成的二维模型(如图 1 所示)，其中保障是由资格保障要求和组织保障要求构成，实施是由工程实施要求和项目实施要求构成。资格保障要求表示一定能力级别所应具备的乙方或与工程相关第三方的资质要求；组织保障要求表示信息安全工程过程要求中对甲方组织保障的要求；工程实施要求表示对信息安全工程中安全过程的要求；项目实施要求表示信息安全工程的项目实施过程要求。

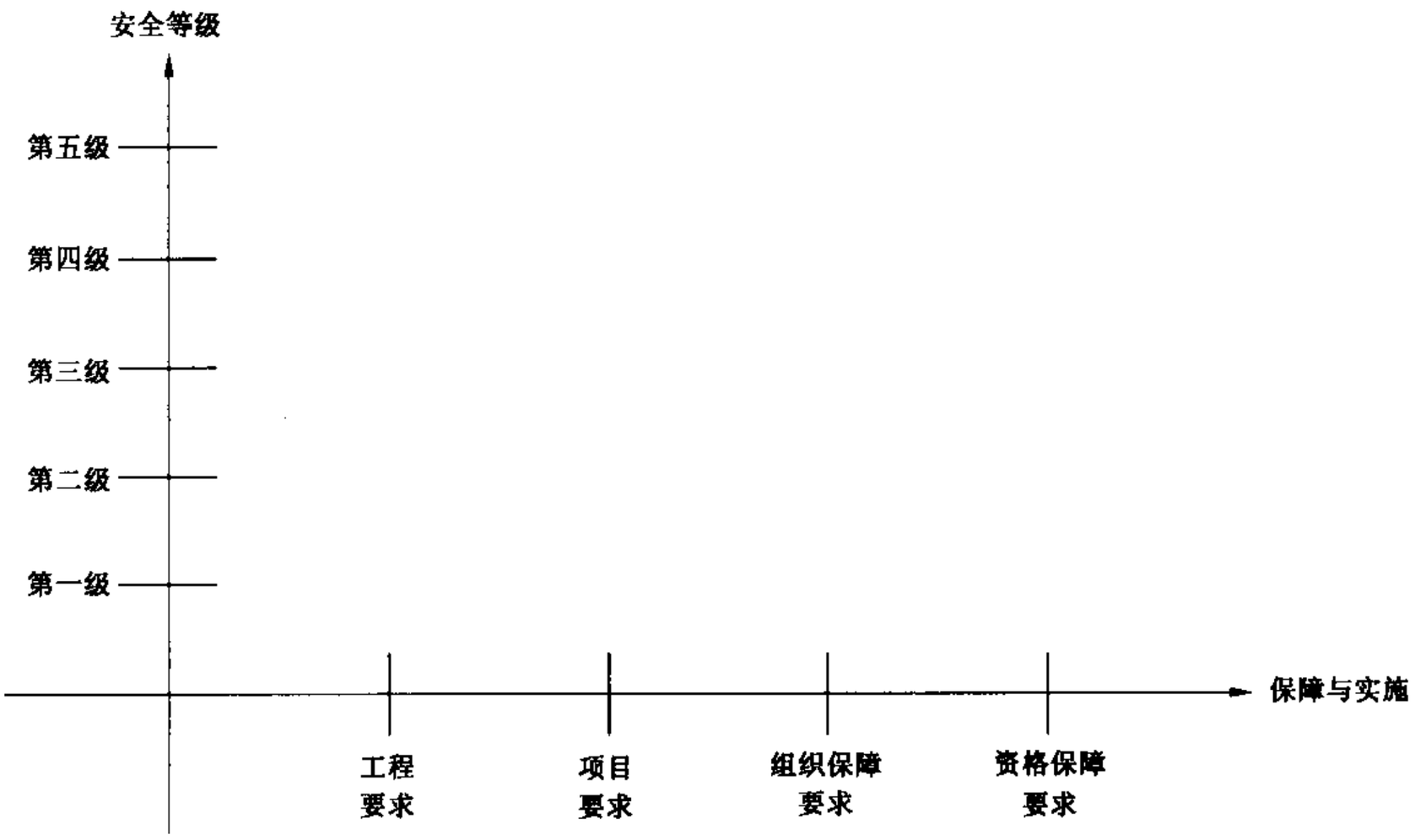

图 1 安全工程等级保护模型

5 资格保障要求

5.1 系统集成资质要求

5.1.1 国家主管部门认可一级集成资质。

5.1.2 国家主管部门认可二级集成资质。

5.1.3 国家主管部门认可三级集成资质。

5.1.4 国家主管部门认可四级集成资质。

5.2 人员资质要求

公安部认可服务人员资质。

5.3 第三方服务要求

5.3.1 公安部认可一级服务单位资质。

5.3.2 公安部认可二级服务单位资质。

5.3.3 公安部认可三级服务单位资质。

5.3.4 公安部认可四级服务单位资质。

5.3.5 公安部认可五级服务单位资质。

5.4 **安全产品要求**

5.4.1 信息安全产品应具有在国内生产、经营、销售的许可证。

5.4.2 操作系统符合保护等级操作系统同级要求。

5.5 **工程监理要求**

5.5.1 应具备信息安全系统建设工程实施监理管理制度。

5.5.2 系统聘请专业监理公司，且监理公司具有国家主管部门认可监理资质证书。

5.6 **密码管理要求**

5.6.1 符合国家密码主管部门的要求。

5.6.2 使用的密码产品为国家主管部门批准的密码产品。

5.6.3 密码产品来源为国家主管部门批准的定点销售单位产品。

5.6.4 使用的密码产品研制来源于国家主管部门批准的密码研制单位。

5.7 **其他要求**

系统符合公共安全的相关法律、法规，按照相关主管部门的技术管理规定手段对非法信息和恶意代码进行有效控制，按照有关规定对设备进行控制使之不被作为非法攻击源或跳板。

6 组织保障要求

6.1 **定义组织的系统工程过程**

6.1.1 **制定过程目标**

6.1.1.1 从组织的应用目标出发为组织的系统工程过程制定目标。

6.1.1.2 系统工程过程在商务环境中运行，为了使组织的标准实现制度化，该目标应得到明确的认可；这个过程的目标应考虑财力、质量、人力资源和对业务成功起重要作用的问题。

6.1.2 **收集过程资产**

6.1.2.1 收集和维护系统工程过程资产。

6.1.2.2 在组织和项目层次中，由过程定义活动所产生的信息都需要存储(在过程资产库中)，使得那些剪裁、过程设计活动中的资产能被使用人理解，并得到维护与保持。

6.1.3 **开发组织的系统工程过程**

6.1.3.1 为组织开发一个充分定义的标准系统工程过程。

6.1.3.2 在开发组织的标准系统工程过程中，可能使用到过程资产库中的设备；在开发任务时，可能需要一些新的过程资产，应该将这些资产添加到过程资产库中；应该将组织的标准系统工程过程置于过程资产库中。

6.1.4 **定义剪裁指南**

定义剪裁组织的标准系统工程过程的指南，该指南在开发项目的定义过程中使用。

6.2 **改进组织的系统工程过程**

6.2.1 **概要**

本要求项包括在组织中用以测量和改进系统工程过程执行的连续活动，利用组织过程资产的初始收集和组织的标准系统工程过程的定义，通过不断改进组织使用的系统工程过程的有效性和效率以获得更大的竞争优势。

6.2.2 **评定过程**

6.2.2.1 评定组织中现有的执行过程以便了解它们的强项和弱项，了解组织现有的执行过程的强项和弱项是建立改进活动基线的关键。

6.2.2.2 评定时应考虑过程执行的测量与课程学习过程；评定可以多种形式进行，评定方法的选择应与文化和组织需求相匹配。

6.2.3 **规划过程改进**

应基于对潜在改进所产生影响的分析，为组织制订过程改进计划，以达到过程的目标。

6.2.4 改变标准过程

改变组织的标准系统工程过程以便反映目标的改进。

6.2.5 沟通过程改进

适当地同现有项目和其他有相关团体共同沟通过程的改进。

6.3 管理系列产品进化

6.3.1 概要

应通过引进服务、设备和新技术以达到产品更新、减少工程费用的目的，达到工程进度和执行的最佳收益，与产品系列一同向其最终目标进化发展。

6.3.2 定义产品进化

6.3.2.1 定义要提供产品的类型。

6.3.2.2 定义支持组织战略目标的系列产品。

6.3.2.3 考虑组织的强项和弱项、竞争力、潜在的市场份额和可利用的技术。

6.3.3 标识新生产技术

6.3.3.1 标识新生产技术或加强基础设施建设，将有助于组织获取、开发和应用新生产技术来提高竞争优势。

6.3.3.2 确定可能引入到系列产品的新生产技术，为确定新技术和基础设施改进而建立并能维护的原始资料和方法。

6.3.4 适应开发过程

6.3.4.1 在产品开发周期中采取必要的变动以支持新产品的开发。

6.3.4.2 适应组织的产品开发过程，熟悉并利用准备在将来使用的组件。

6.3.5 确保关键组件的可用性

6.3.5.1 确保关键组件都可利用，并可以支持有计划的产品改进。

6.3.5.2 组织应决定产品系列的关键组件及其可用性的计划。

6.3.6 插入产品技术

6.3.6.1 将新的技术插入到产品开发、市场营销和制造过程中。

6.3.6.2 管理将新技术引入到系列产品的工作(包括现有产品系列组件的改进、新组件的引进)；标识和管理与产品设计变化有关的风险。

6.4 管理系统工程支持环境

6.4.1 概要

本要求项列出了在项目层面和组织层面都属于系统工程支持环境的事项。支持环境的元素由系统工程活动的所有环境组成，包括：计算机资源、网络带宽、分析方法、组织结构策略和程序、机器的购买、化学处理设施、环境强调设施、系统工程仿真工具、软件开发工具、专有的系统工程工具、工作空间等。

6.4.2 维持技术认识

6.4.2.1 维持对支持实现组织目标的那些技术的认识。

6.4.2.2 对工艺现状或实施现状应该插入新的技术，组织应具有对新技术的充分认识。

6.4.3 确定支持需求

根据组织的需要确定组织的系统工程支持环境的需求。

6.4.4 获得系统工程支持环境

6.4.4.1 获得一个系统工程支持环境，该环境要满足在确定支持需求中通过利用分析候选解决要求项的实施而建立的要求。

6.4.4.2 针对所需的系统工程支持环境，确定其评价标准和潜在的候选解决方案；利用分析候选解决要求项选择一个解决方案；得到并实现所选的系统工程支持环境。

6.4.5 **剪裁系统工程支持环境**

剪裁系统工程支持环境，以满足单个项目的要求。

6.4.6 **插入新技术**

6.4.6.1 根据组织的应用目标和项目需要将新技术插入到系统工程支持环境中。

6.4.6.2 组织的系统工程支持环境应用新技术更新，并要支持组织的应用目标及工程需要；在系统工程支持环境中，应提供使用新技术的培训。

6.4.7 **维护环境**

6.4.7.1 维护系统工程支持环境以持续支持依赖该环境的项目。

6.4.7.2 维护活动包括计算机系统管理、培训、热线支持、专家的作用、发展或者扩充一个技术库等。

6.4.8 **监视系统工程支持环境**

6.4.8.1 监视系统工程支持环境以发现改进的机会。

6.4.8.2 确定影响系统工程支持环境有用性的因素，包括任何新插入的技术；监视新技术和整个系统工程支持环境的接受情况。

6.5 **培训**

6.5.1 **确定培训要求**

6.5.1.1 以项目的要求、组织的战略计划和现有的员工技能情况为指导，确定组织在技能与知识方面所需的改进。

6.5.1.2 综合现有的程序、组织的战略计划和现有员工的技能等各方面信息确定这些要求。

6.5.2 **选择知识或技能的获取模式**

6.5.2.1 评价和选择通过培训或其他资源获取知识或技能的适当模式。

6.5.2.2 应确保所选择的方法是最佳的，以使得所需技能和知识对项目及时有效。

6.5.3 **确保技能和知识的可用性**

确保技能和知识对系统工程活动是适用的。

6.5.4 **准备培训材料**

6.5.4.1 根据确定的培训要求准备培训材料。

6.5.4.2 为每一个由组织内部人员建成的班编制培训材料，或为每一个已存在的班准备培训材料。

6.5.5 **培训人员**

6.5.5.1 培训教员要具备执行赋予他们的角色的技能与知识。

6.5.5.2 要根据培训计划和编制的材料进行人员培训。

6.5.6 **评估培训的有效性**

6.5.6.1 评估培训的有效性以满足所确定的培训要求。

6.5.6.2 评估有效性的方法应与培训计划编制和培训材料的拟定同时列出；应及时获取有效性评估的结果，以便对培训做出相应调整。

6.5.7 **维护培训记录**

6.5.7.1 维护培训与取得经验的记录。

6.5.7.2 维护记录以追踪每个人员接受培训的情况，以及受训后的技能和能力。

6.5.8 **维护培训材料**

6.5.8.1 维护知识库中的培训材料。

6.5.8.2 维护知识库中的课件材料以供员工今后访问，并且在课程材料变动时可供跟踪。

6.6 **与供应商协调**

6.6.1 **确定系统的组件或服务**

确定应由其他外部组织提供的系统组件或服务。

6.6.2 **确定胜任的供应商或销售商**

6.6.2.1 标识在特定领域中具有专门技术的供应商。

6.6.2.2 供应商的能力包括胜任开发过程、制造过程、验证责任、及时交付、生命期支持过程，以及远程有效通信能力，上述能力应符合本组织的各项要求。

6.6.3 选择供应商或销售商

6.6.3.1 依照要求项(7.1)选择供应商。

6.6.3.2 以合乎逻辑和公平的方式选择供应商以满足产品的目标；提供最能弥补本组织能力的供应商特征，识别合格的候选者；利用要求项(7.1)的实施来选择出合适的供应商。

6.6.4 提供期望

6.6.4.1 对供应商提出组织对系统组件或服务的要求、期望和效果指标。

6.6.4.2 在合同签署时组织应将它的要求和期望清楚地指明并排出优先顺序，并且要指明对供应商方面的所有限制；组织要与供应商密切合作，使其充分了解产品达到的要求和自己要承担的责任，并达成相互理解。

6.6.5 维持沟通

6.6.5.1 与供应商维持及时的双向沟通。

6.6.5.2 组织与供应商要对期望的和所需的沟通建立相互谅解。所建立的沟通的特点包括：双方公认的公开的没有任何限制的信息类型，受限的信息类型(如策略或合同关系)，所期望的信息请求与回应的及时性，用于沟通的工具和方法，安全，保密以及期望的分布情况。

7 工程实施要求

7.1 管理安全控制

7.1.1 概要

应保证系统在运行状态下达到设计预期的安全特性，安全控制措施被配置且能正常使用。

7.1.2 建立安全职责

7.1.2.1 建立安全控制措施的职责和责任并通知到组织中的每一个人。

7.1.2.2 本项目应该保证承担相应安全责任的人员是负责的，并获得相应的授权；应该保证采用的所有安全控制措施是明确的，并被广泛和一致地应用。

7.1.3 管理安全措施的配置

7.1.3.1 所有设备的安全配置都需要管理。

7.1.3.2 管理系统安全控制措施的配置。

7.1.4 管理安全意识、培训和教育大纲

7.1.4.1 组织和管理对所有员工进行安全意识的培训和教育。

7.1.4.2 管理所有的用户和管理员的安全意识、培训和教育大纲。

7.1.5 管理安全服务及控制机制

7.1.5.1 安全服务及控制机制的一般管理类似于其他服务及机制的管理，包括保护它们避免损伤、偶然事故和人为故障，并根据法律和政策要求进行整理并归档。

7.1.5.2 对安全服务及控制机制进行定期的维护和管理。

7.2 评估影响

7.2.1 概要

应识别对该系统有关系的影响，并对发生影响的可能性进行评估。

7.2.2 对影响进行优先级排列

对在系统中起关键作用的运行、商务或任务的能力进行识别、分析和按优先级排列。

7.2.3 识别系统资产

7.2.3.1 对支持系统的安全目标或关键性能力(运行、商务或任务功能)进行识别。

7.2.3.2 对必需的系统资源和数据进行识别;通过对给定环境中提供这种支持的每项资产的意义进行评估,来对每项资产进行定义。

7.2.3.3 对支持系统的关键性运行能力或安全目标的系统资产进行识别和特征化。

7.2.4 选择影响的度量

应预先确定适合的度量用于评估影响。

7.2.5 标识度量关系

标识所选影响的评估度量与度量转换因子之间的关系。

7.2.6 识别和特征化影响

利用多重度量或统一度量的方法对意外事件的意外影响进行识别和特征化。

7.2.7 监视影响

监视影响中的变化,本条与 7.8.3 中的通用性监视活动紧密相连。

7.3 评估安全风险

7.3.1 概要

通过对在一给定环境中运行该系统相关的安全风险的理解,并按照给定的方法论对风险问题进行优先级排序。

7.3.2 选择风险分析方法

7.3.2.1 本要求项包括定义用于识别给定环境中的系统安全风险的方法,该方法是对安全风险进行分析、评估和比较;应该包括一个对风险进行分类和分级的方案,其依据是威胁、运行功能、已建立的系统脆弱性、潜在损失、安全需求等相关问题。

7.3.2.2 选择用于分析、评估和比较给定环境中系统安全风险所依据的方法、技术和准则。

7.3.3 识别风险

7.3.3.1 识别该风险,认识这些威胁和脆弱性的利害关系,进而识别出威胁和脆弱性造成的影响;这些风险在选择系统保护措施中应予以考虑。

7.3.3.2 识别威胁/脆弱性/影响三组合(风险)。

7.3.4 评估风险

7.3.4.1 识别每个风险出现的可能性。

7.3.4.2 评估与每个风险有关的风险。

7.3.5 评估总体不确定性

7.3.5.1 每种风险都有与之相关的不确定性;总体风险不确定性是在 7.4.6 中已被标识的威胁、脆弱性和影响及其特征不确定性的积累、7.4.6、7.5.4 以及 7.3.6。本要求项与 7.6 密切相关,因为证据能用于追踪修改,从而在某种输入下降低不确定性。

7.3.5.2 评估与该风险有关的总体不确定性。

7.3.6 风险优先级排列

7.3.6.1 已经被识别的风险应以组织优先权、风险出现的可能性与这些因素相关的不确定性和可用财力为依据进行排序;风险可以被减轻、避免、转移或接受,也可以使用这些措施的组合。“减轻”这一措施能够对付威胁、脆弱性、影响或风险本身;安全措施的选择要适当考虑到 7.10“指定安全要求”中的要求,商务优先级和整个系统体系结构。

7.3.6.2 按优先级对风险进行排列。

7.3.7 监视风险及其特征

7.3.7.1 定期地检查新的风险,本条与 7.8.3“监视威胁、脆弱性、影响、风险和环境方面的变化”中一般性监视活动紧密相联。

7.3.7.2 监视风险频率变化和风险特征的变化。

7.4 评估威胁

7.4.1 **概要**

应识别安全威胁及其性质和特征，对系统安全的威胁进行标识和特征化；应定期地对威胁进行监视，以保证由本要求项所产生的安全理解始终得到维持。

7.4.2 **识别自然威胁**

识别由自然原因引起的相应威胁。

7.4.3 **识别人为威胁**

识别由人为偶然原因引起的威胁与故意行为引起的威胁。

7.4.4 **识别威胁的测量尺度**

7.4.4.1 对可能在特定位置中出现的预料中事件，应根据具体情况建立最大和最小测量单位范围。

7.4.4.2 识别特定环境中适当的测量尺度和适用范围。

7.4.5 **评估威胁影响的效果**

7.4.5.1 确定对系统进行成功攻击的黑客潜在的能力。

7.4.5.2 评估由人为原因引起的威胁影响的动因和结果。

7.4.6 **评估威胁的可能性**

对威胁事件如何发生的可能性进行评估，评估出现威胁事件的可能性。

7.4.7 **监视威胁及其特征**

7.4.7.1 有规律地对现有威胁及其特征进行监视，并检查新的威胁；本条与 7.8.3 的一般化监视活动紧密相连。

7.4.7.2 监视威胁频谱中不断的变化以及相应特征的变化。

7.5 **评估脆弱性**

7.5.1 **概要**

应识别和特征化系统的安全脆弱性。本要求项包括分析系统资产、定义特殊的脆弱性以及提供对整个系统脆弱性的评估，并获得对一确定环境中系统安全脆弱性的理解。

7.5.2 **选择脆弱性分析方法**

7.5.2.1 所有分析应在预先安排和指定时间内，在一个已知的并记录有配置的框架内进行；分析的方法论应包括预期结果；分析的特定目标应陈述清楚。

7.5.2.2 选择对一确定环境中系统安全脆弱性进行识别和特征化的方法、技术和标准。

7.5.3 **识别脆弱性**

7.5.2 中研究过的脆弱性分析方法论应延伸到对脆弱性的证实；所有发现的系统安全脆弱性应予以记录、识别。

7.5.4 **收集脆弱性数据**

收集与脆弱性相关的数据。

7.5.5 **综合系统脆弱性**

分析哪些脆弱性或脆弱性的组合会对系统造成问题，所有分析应识别出该脆弱性的特征；评估由特定脆弱性和特定脆弱性组合所产生的系统脆弱性与总体脆弱性。

7.5.6 **监视脆弱性及其特征**

7.5.6.1 本项要求与 7.8.3 的变化的一般性监视活动紧密相连。

7.5.6.2 监视脆弱性及其特征的连续变化。

7.6 **建立保证论据**

7.6.1 **概要**

本项目包括对与需求有关的保证进行识别和定义，包括证据的产生和分析的活动，包括支持保证需求所需的附加证据、文档清单和过程以及那些能清晰地向用户提供已满足其安全需求的证据。

本项目要求建立保证证据有关的活动记录，包括管理、标识、计划、封装和提交安全保证证据。

7.6.2 识别保证目标

7.6.2.1 识别安全保证目标。

7.6.2.2 系统安全保证目标应规定强制性系统安全策略的机密性等级；目标的充分性由开发者、集成者、用户和签名授权者确定。

7.6.2.3 新的和修改过的安全保证目标的标识应与所有内部和外部工程组织等安全相关性团体保持协调一致。

7.6.2.4 对安全保证目标进行修改的内容需及时解释其中变化。

7.6.2.5 安全保证目标应清晰地沟通。

7.6.3 定义保证策略

7.6.3.1 规划并确保正确地实现强制性安全目标；通过实现安全保证策略所产生的证据应(向系统签名授权者)提供一个可接受的机密性等级，此等级安全的测量足以管理安全风险。通过开发并颁布安全保证策略，获得对保证的相关活动进行有效管理；工程早期应对需求相关的保证进行的识别和定义产生必要的支持证据；通过不断外部协调，对保证用户需求的满意程度进行理解和监视，确保高质量组合保证要求。

7.6.3.2 为所有保证目标定义一个安全保证策略。

7.6.4 控制保证证据

安全保证证据通过与所有工程实施要求项相互配合，在安全保证策略内识别出的不同层面抽象的证据的方法进行收集；证据应受到控制。

7.6.5 分析证据

对安全保证证据进行分析，保证工程产品相对于基线系统是完善和正确的。

7.6.6 提供保证论据

7.6.6.1 开发出一个完整的证明与安全目标一致的安全保证论据，并提供给用户；保证论据是由多层抽象中获得的保证证据的组合所支持的一系列声明性保证目标；应对提交证据中的缺陷和安全保证目标中的缺陷进行复查。

7.6.6.2 提供证明用户安全需求得到满足的安全保证性论据。

7.7 协调安全

7.7.1 概要

保证所有部门都有一种参与安全工程的意识，协调并保持所涉及到安全组织、其他工程组织和外部组织之间的关系；多种机制用于在这些部门之间协调和沟通安全工程的决定和建议，包括备忘录、文档、电子邮件、会议和工作组。

项目组的所有成员应具有参与安全工程工作的意识，有关安全的决策和建议是相互沟通和协调一致的结果。

专业的安全工程师应该是所有主要设计队伍和工作组、开发和运行机构；在做出关键设计决定后的工程生命期早期应建立起安全工程与其他工程队伍间的联系。

7.7.2 定义协调目标

定义和建立与其他组织之间的联系和义务关系；这些关系应被全体参与部门所接受。

7.7.3 识别协调机制

识别安全工程的协调机制，明确协调机制实现的方法。

7.7.4 促进协调

7.7.4.1 确保不同优先级的不同组织间进行沟通有可能发生的一些冲突和争端以合适的、富有成果的方式得到解决。

7.7.4.2 促进安全工程的协调。

7.7.5 协调安全决定和建议

在各种安全工程组织、其他工程组织、外部实体及其他合适的部门中沟通安全决定和建议，用识别出的机制去协调有关安全的决定和建议。

7.8 监视安全态势

7.8.1 概要

确保识别并报告所有的安全违规行为；监视外部和内部环境中可能影响系统安全的所有因素；探测和跟踪内部和外部与安全有关的事件。根据策略制定响应突发事件的措施；根据安全目标识别并处理运行安全态势的变化。

7.8.2 分析事件记录

检测安全相关性信息的历史和事件记录，通过多条记录中的事件相关元素，识别出安全事件；分析事件记录，以确定事件的原因、预测可能发生的事件。

7.8.3 监视变化

监视威胁、脆弱性、影响、风险和环境方面的变化，查找可能影响当前安全状态有效性的任何变化：监视所有因素的变化并分析这些变化以评估它们对安全有效性的意义。

7.8.4 识别安全突发事件

7.8.4.1 确定是否发生了一个有关安全的突发事件，识别出事件详细情况并且在必要时提出报告；有关安全的突发事件可利用历史事件的数据、系统配置数据、完整性工具和其他系统信息诊断。

7.8.4.2 识别与安全相关的突发事件。

7.8.5 监视安全防护措施

7.8.5.1 检测安全防护措施的执行情况，识别出安全防护措施执行中的变化。

7.8.5.2 监视安全防护措施的性能和有效性。

7.8.6 检查安全态势

检查系统安全态势以识别出必要的更正，复查实施安全的理由并根据其他的规则检查需要安全的地方。

7.8.7 管理安全突发事件响应

应急计划要求识别出系统失效的最长时间、系统正常工作的基本元素；开发一个可恢复策略和计划，测试并维护该计划。

7.8.8 保护安全监视的记录数据

保证与安全监视有关的设备得到适当的保护，监视活动包括封存和归档相关的日志、审计报告和相关分析结果。

7.9 提供安全输入

7.9.1 概要

为系统的规划者、设计者、实施者或用户提供他们所需的安全信息，信息应包括安全体系结构、设计或实施选择以及安全指南；开发、分析并提供安全输入并与基于 7.10“指定安全要求”中定义的安全需求中的适当组织机构成员协调一致；要求所有具有安全意义的系统问题都应受到检查并按照安全目标的要求予以解决；所有项目组成员都要理解安全问题，解决方法应反映出所提供的安全输入。

本要求项适用于标定开发(设计者和实现者)和运行(用户和管理员)的安全输入。

7.9.2 理解安全输入要求

7.9.2.1 安全输入包括任何种类的、应被其他项目所考虑的、与安全相关的指南、设计、文档或思想；输入可以为多种形式包括文档、备忘录、电子邮件、培训和咨询。

7.9.2.2 安全输入要求可基于 7.10 中确定的需求。

7.9.2.3 设计者、开发者和用户应一起确保相应部门对安全输入有一个共同的理解。

7.9.3 确定安全约束和考虑

确定做出有科学依据的工程决策所需的所有安全约束和考虑。安全工程组进行分析以决定在需

求、设计、实现、配置和文档方面的任何安全限制和考虑；约束可在系统生命期内的所有时间进行标识，可在许多不同的抽象层上进行标识。

7.9.4 识别安全选项

识别出与安全相关的工程问题的解决办法选项；解决办法可以多种形式提供。

7.9.5 分析工程选项的安全性

7.9.5.1 分析和区分工程选项的优先级；确定安全约束同时考虑(7.9.3)，根据识别的安全约束和考虑结果，设计组可以评估每个工程选项并提出对工程组的建议；安全工程组应考虑其他工程组的工程指南。

7.9.5.2 这些工程选项不受所标识的安全选项的限制(7.9.4)，还应包括来自其他项目的选项。

7.9.5.3 利用安全约束和考虑来分析和区分工程选项的优先级。

7.9.6 提供安全工程指南

制定出与安全相关的指南，并将它提供给工程组。

7.9.7 提供运行安全指南

7.9.7.1 制定出与安全相关的指南并提供给系统用户和管理员；运行安全指南的制定应在生命期内提早开始。

7.9.7.2 运行安全指南包含用户和管理员在以安全模式进行安装、配置、运行和终止系统时应做的内容。

7.10 指定安全要求

7.10.1 概要

明确地为系统识别出与安全相关的要求；指定安全要求涉及到系统安全定义的基本原则，遵循有关安全的所有法律、策略和组织需求；定义与安全相关的要求集合成系统安全的基线。

所有部门，包括用户之间应达成对安全要求的共识。

定义整个信息系统中所有安全方面的活动，通过在整个项目中收集、提炼、使用和更新(详见7.9)这一要求项所获得和产生的信息，提出安全要求。

7.10.2 获得对安全要求的理解

通过收集所有用于全面理解用户安全要求所需的信息，获得对安全要求的理解。

7.10.3 识别可用的法律、策略和约束

为给定系统确定法律、策略、标准、外部影响和约束；收集所有对系统安全产生影响的外部影响；识别出支配系统目标环境的法律、规则、策略和商务标准；应进行全局和局部间优先级的决策；系统用户提出的系统安全需求应被标识并说明安全意义。

7.10.4 识别系统安全关联性

7.10.4.1 识别出系统间的关系是如何影响安全的，任务的处理和运行概要应作为安全因素加以评估；识别对系统遭受到的或可能遭受到的威胁，评估性能和功能需求对安全可能产生的影响。

7.10.4.2 定义系统的安全边界；组织的许多外部因素也影响组织安全要求的变化程度，监视和定期地评估策略上的倾向性和策略重点的改变、技术开发、经济影响、全局性事件以及信息战等变化带来的潜在影响。

7.10.4.3 识别系统的用途以确定其安全的关联性。

7.10.5 获取系统运行的安全思想

7.10.5.1 应明确总体的、面向安全的指导思想，包括任务、职责信息流、资产、资源、人员保护以及物理保护的指导思想。

7.10.5.2 明确系统运行的面向安全的总体指导思想。

7.10.6 获取安全的高层目标

确定在运行环境中对系统安全性是足够的安全目标；获取高层安全目标就是定义系统的安全性。

7.10.7 定义安全相关需求

7.10.7.1 定义与系统安全相关的需求，应保证需求的完备性和一致性，为系统安全的评价提供基础。

7.10.7.2 定义一套一致性需求，该需求定义了在系统中将实现的保护。

7.10.8 达成安全协议

应在系统的安全需求中将所有的适用部分与特定安全之间达成协议；对于未被识别的特殊用户而不是一个通用用户组的情况下，特定安全要满足目标设置；特定的安全应该完整地、一致地反映出对策略、法律和用户需求的管理；应识别并修改所发现的问题，直到达成满足用户要求的协议。

7.11 验证和证实安全性

7.11.1 概要

确保解决安全问题的办法已经被验证与证实。通过观察、示范、分析和测试，依照安全需求、体系结构和设计确认解决办法；依照用户的运行安全需求证实解决办法；解决办法应满足用户安全需求与运行安全要求。

7.11.2 确定验证和证实的目标

确定验证和证实的目标；确定验证和证实的解决办法。

7.11.3 定义验证和证实方法

7.11.3.1 应定义验证和证实每种解决方案的方法和严密等级；

7.11.3.2 严密等级应表明验证和证实的审查到底应有多严格；该要求项要受到 7.6 中保证策略输出的影响。

7.11.4 执行验证

7.11.4.1 应通过显示解决办法实现与上一抽象层相关的要求，包括确定的保证需求正是作为 7.6 的结果所识别的保证需要；所用的方法在 7.11.3 中有标识；个人需求和整个系统都要受到检测。

7.11.4.2 验证解决办法实现了与上一抽象层相关的要求。

7.11.5 执行证实

7.11.5.1 通过显示能满足与上一抽象层相关的要求，最终满足用户的运行安全要求，实现对解决办法的证实。

7.11.5.2 证实解决办法满足与上一抽象层关联的需要；所使用的方法应在 7.11.3 中确定。

7.11.6 提供验证和证实的结果

为其他工程组收集并提供验证和证实的结果；验证和证实的结果应以某种易被理解和使用的方式所提供；所有结果应被跟踪。

8 项目实施要求

8.1 概要

计算机信息系统安全工程等级项目保证过程就是计算机信息系统安全保护等级要求包括一些附加注释以说明与安全工程项目有关的过程。这些注释都包含在每一个计算机信息系统安全保护等级要求项目的开头部分中。

8.2 质量保证

8.2.1 概要

本要求项与 7.6“建立保证论据”有关。保证可以认为是安全相关质量的特殊类型。

8.2.2 监视所定义过程的一致性

8.2.2.1 确保项目是按照所定义的系统工程过程来执行的；应按适当的时间间隔来检查一致情况；应将与所定义的过程相偏离以及该偏离所带来的影响记录下来。

8.2.2.2 确保所定义的系统工程过程在系统生命期中是稳定的。

8.2.3 测量工作产品的质量

8.2.3.1 应当运用所设计的测量工作产品的方法来评估工作产品是否能符合用户或工程的要求;产品测量还有助于解决隔离系统开发过程中的问题。

8.2.3.2 根据工作产品的质量要求对工作产品的测量进行评价。

8.2.4 测量过程质量

对项目所使用的系统工程过程的质量进行测量。

8.2.5 分析质量测量

8.2.5.1 分析质量测量以对质量改进或操作改进方面提出适当的开发性建议。

8.2.5.2 绘制因果图。

8.2.6 参与

在确定和报告质量问题时,有关员工应参与其中。

8.2.7 发起改进质量的活动

应发起以质量问题或质量改进问题为主题的有关活动。

8.2.8 检测修正行为要求

8.2.8.1 建立一种或一套机制来检测过程或产品中修正行为的要求。

8.2.8.2 故障报告。

8.3 管理配置

8.3.1 概要

应维持已确定的配置单元的数据和状况,并对系统及其配置单元的变化进行分析和控制;管理系统配置包括为开发者和用户提供准确的当前配置数据和状况;该要求项对置于配置管理之下的所有工作产品都是适用的。

在8.3中对一个系统/项目而标识的配置单元级别的确定应当考虑7.6的保证目标所详细要求的级别。

管理配置提供了7.6的证据;选择的配置管理(CM)系统自身管理也应当通过7.1“管理安全控制”来管理。

配置管理功能应允许在配置生命期的任一点上通过系统要求的层次来对配置进行跟踪,从而支持可追溯性;可追溯性作为要求项(8.3)中实施的一部分应建立起来。

8.3.2 建立配置管理方法

8.3.2.1 应有配置管理方法;

8.3.2.2 应将要求项(8.2)作为实现业务研究的指南。

8.3.2.3 配置管理过程的描述。

8.3.3 确定配置单元

8.3.3.1 确定构成基线的配置单元。

8.3.3.2 配置管理所选择的工作产品应基于所选配置管理策略建立的准则上;配置单元应当在有利于开发者和用户的层面之上进行选择,但不应将不合理的管理负担加在开发者的身上。

8.3.4 维护工作产品基线

维护工作产品基线库,建立和维护一个关于工作产品配置的信息库;维护配置数据,为审计跟踪提供在系统生命期任一点上的原始资料。

8.3.5 控制变化

8.3.5.1 对已建立的配置项的变化进行控制,包括跟踪每个配置项的配置;如需要批准新的配置,应更新系统的基线。

8.3.5.2 应对工作产品的标识问题或改变工作产品的需求进行分析,以便确定此变化对工作产品、项目进度和费用、以及其他工作产品产生的影响。

8.3.6 沟通配置状况

在状况发生变化时，应将配置数据状况告诉相关的部门或人员。状况报告应当包含何时处理、已接受的配置单元变化和受变化影响的有关工作产品等信息；应为开发者、用户和其他受影响的团体提供配置数据和状况的访问权利。

8.4 管理项目风险

8.4.1 概要

应标识、评估、监视和降低风险以使系统工程活动和全部技术活动均取得成功；这个要求项要持续整个工程生命期。与(8.6)和(8.5)要求项相类似，本要求项的范围包括系统工程活动和全部技术项目活动。

“项目风险”指与项目成功完成有关的风险，与费用和进度有关的一系列问题。工程实施要求项列出 “安全风险”活动，这些活动是用来决定是否可容忍残余安全脆弱性对运行的影响。

应当考虑到 7.7，以确保安全问题都已列出。

8.4.2 制定风险管理方法

8.4.2.1 为风险管理活动制定出一个计划，对于整个项目生命期来说，该计划是标识、评估、降低和监视风险的基础。

8.4.2.2 本要求实施的目的是制定一个有效的计划以指导项目的风险管理活动；计划元素应当包括风险管理队伍成员的标识及其责任；应有用于标识和降低风险的常规风险管理活动、方法和工具列表以及风险降低活动的跟踪和控制方法；计划也应当为风险管理结果的评估提供帮助。

8.4.3 标识风险

8.4.3.1 通过检查项目目标(并考虑到选择和限制)确定可能出现哪些错误并以这两种方法来标识项目的风险。

8.4.3.2 有条理地审查项目目标、项目计划(包括活动或事件依赖性)以及系统需求，确定可能的困难区以及在这些区中会出现哪些错误；上述活动在要求项(8.6)中制定；建立关键的发展依赖性和提供跟踪和修正行为将在要求项(8.5)中完成。

8.4.4 评估风险

评估风险，确定风险发生的可能性与可能造成的后果。

8.4.5 复查风险评估

8.4.5.1 获得项目风险评估的正式认可。

8.4.5.2 复查风险评估的充分性，以决定是否需要修改或取消基于风险的承诺。

8.4.6 执行风险降低活动

8.4.6.1 实施风险降低活动。

8.4.6.2 可列出风险降低活动减少风险发生的可能性或减少风险发生时所造成损失程度的列表；对需要特别关注的风险，可以同时实施几种降低风险的活动。

8.4.7 跟踪风险降低活动

8.4.7.1 监视风险降低活动以确保得到预期结果。

8.4.7.2 定期检查已经有效实施的降低风险活动，测量结果并确定该活动是否成功。

8.5 监控技术活动

8.5.1 概要

应为实际进步和风险提供充分的可见性；可见性是在执行计划发生严重偏差时及时促进修正的行为。

“监控技术活动”将根据项目估计、承诺和计划的文档来指导、跟踪和复查项目的完成情况、结果和风险；一个计划的文档是用来作为跟踪活动和风险，交流情况和修改方案的基础。

类似于要求项(8.6)，此要求项适用于项目技术性行为以及系统工程活动。

在开发和系统运行时，需要考虑到 7.8 和 7.1。

需要考虑到要求项(7.7)以确保安全问题都已经列出。

8.5.2 指导技术活动

8.5.2.1 根据技术性管理计划指导技术性活动。

8.5.2.2 贯彻落实在“计划技术活动”要求项中创建的技术管理计划;这一实施涉及到项目中所有工程活动的技术指导。

8.5.3 跟踪项目资源

8.5.3.1 根据技术性管理计划跟踪资源的实际利用情况。

8.5.3.2 提供在项目中资源使用的当前信息,在需要时及时调整活动和计划。

8.5.4 跟踪技术参数

8.5.4.1 根据已建立的技术性参数跟踪执行。

8.5.4.2 通过测量在技术管理计划中建立的技术性参数来跟踪项目和它的产品的实际执行;将测量结果与技术管理方案中建立的阈值进行比较,将问题通知给管理人员。

8.5.5 复查项目执行

8.5.5.1 根据技术性管理计划执行复查。

8.5.5.2 应定期对项目和其产品的执行情况进行复查,当超出正常技术参数的阈值时也要进行复查;复查技术执行的测量分析结果和技术执行的其他指标,批准修正行动计划。

8.5.6 分析项目问题

8.5.6.1 分析跟踪和复查技术性参数的结果,决定修正行动。

8.5.6.2 及时标识、分析和跟踪项目问题控制项目的执行。

8.5.7 采取修正行动

8.5.7.1 当实际结果偏离计划时或技术参数预示着将有问题时,应采取修正行动。

8.5.7.2 当修正行动批准后,通过再分配资源,改变方法和步骤或加强对原计划的支持来执行修正行动;当需要改变技术管理计划时,采用(8.6)以修改该计划。

8.6 计划技术活动

8.6.1 概要

应建立计划,这些计划能为在系统开发、制造、使用和配置过程中涉及到的技术性工作的进度、费用、控制、跟踪与商议的性质和范围提供基础;应将系统工程行为集成到整个项目的综合性技术计划中。

“计划技术活动”涉及对所要执行工作量的估算,从有相关的部门或人员中获得必要的承诺,并对要进行的工作计划进行定义。

应考虑到 7.7,特别是在执行 8.6.6 和 8.6.7 时。

计划应从对要进行的工作范围的理解开始,然后定义项目的限制和约束、风险和目标;计划过程应包括估算工作产品的规格,估算所需资源,制定时间安排表,考虑风险和协商承诺等步骤。

8.6.2 识别关键资源

识别对项目技术上的成功起关键作用的资源。

8.6.3 估计项目范围

8.6.3.1 对影响项目的规模和技术可行性的因素进行估计。

8.6.3.2 应通过将系统分解成与其他项目相似的组成单元的办法来对项目范围和规模进行估计;对规模的估计可以调整为如复杂性差异或其他参数等因素。

8.6.3.3 历史原始资料可为初始规模估计提供最有用的信息。

8.6.4 估算项目费用

针对项目实施要求的所有技术资源建立费用估算。

8.6.5 确定工程过程

8.6.5.1 确定项目使用的技术过程。

8.6.5.2 在最高层的技术过程应遵循基于工程特征、组织特征和组织的标准过程的生命期模型。

8.6.6 确定技术活动

8.6.6.1 为项目的整个生命期确定技术活动。

8.6.6.2 参照组织的历史经验，从可适用的标准与业界最佳实践中选择项目和系统工程活动。

8.6.7 定义项目界面

定义支持与用户和供应商进行有效交互作用的特定过程。

8.6.8 开发项目进度表

8.6.8.1 为项目的整个生命期制定技术进度表。

8.6.8.2 项目进度表包括系统和组件的开发与采购，相关人员的培训以及工程所需支持环境的准备；进度表是基于可验证模型或已确定任务的数据，以及它们任务相互依赖性和采购项的可用性；进度表应当包括为已标识的风险留有余地；所有受影响的部门或个人应复审并提交该进度表。

8.6.9 设立技术参数

8.6.9.1 为项目和系统设立有阈值的技术参数。

8.6.9.2 设立可在工程整个生命期中都需要跟踪的关键技术参数，这些参数作为进度指示，以便满足最后的技术目标；通过交互用户、用户需求、市场调查、原型、已标识风险或类似项目的历史经验来确定这些关键技术参数。每个可跟踪的技术参数应该有一个期望的校正阈值或公差；在项目进度表中的重要时间点关键技术参数应进行事先估算。

8.6.10 开发技术管理计划

8.6.10.1 利用在计划活动中收集到的信息开发技术管理计划，这种计划可以作为跟踪项目和系统工程的基础。

8.6.10.2 制定并维护所有技术活动需要的内部、外部组织项目活动的完整计划。

8.6.11 复查并认可工程计划

8.6.11.1 与所有有关团体和个人一同复查技术管理计划并需得到团体认可。

8.6.11.2 应确保在整个工程中通过有影响的团体和个人，对过程、资源、进度表和信息需求有自上而下的共同理解。

9 用于工程管理等级划分的要求

9.1 第一级

9.1.1 工程目标和范围

目标：在这一级别，要求满足资格保障的基本要求项，应基本达到组织保障、工程实施和项目实施的基本要求项。此级别组织内的个人可识别出一个行动应被执行，并同意这个行动会在需要时执行。

范围：这个级别应该制定安全工程计划，明确计算机信息系统的安全目标和安全范围并经组织内或具有所有权单位的主管领导批准。

保证计算机信息系统安全保护等级达到 GA/T 390—2002 中 6.1、GA/T 391—2002 中 5.1 的要求。

9.1.2 资格保障要求

a) 5.4.1 国家主管部门认证信息安全产品许可证书的产品；

b) 5.4.2 操作系统符合安全等级保护操作系统同级要求；

c) 5.6.1 符合保护等级密码管理指南同级别要求；

d) 5.6.2 密码产品为国家批准的密码产品；

e) 5.6.3 来源于国家批准的定点销售单位产品；

f) 5.6.4 研制来源于为国家批准的密码研制单位；

g) 5.7 系统符合公共安全的相关法律、法规。

9.1.3 组织保障要求

安全组织保障过程中6个要求项的过程完整、明确，应基本达到每个要求项的目标；此级别组织内的个人可识别出一个行动应被执行，并同意这个行动会在需要时执行。

a) 6.1 定义组织的系统工程过程；

b) 6.2 改进组织的系统工程过程；

c) 6.3 管理系列产品进化；

d) 6.4 管理系统工程支持环境；

e) 6.5 提供不断发展的技能和知识；

f) 6.6 与供应商协调。

9.1.4 工程实施要求

安全工程中11个要求项的过程完整、明确，应基本达到每个要求项的目标；组织内的个人可识别出一个行动应被执行，并同意这个行动会在需要时执行。

a) 7.1 管理安全控制；

b) 7.2 评估影响；

c) 7.3 评估安全风险；

d) 7.4 评估威胁；

e) 7.5 评估脆弱性；

f) 7.6 建立保证论据；

g) 7.7 协调安全；

h) 7.8 监视安全态势；

i) 7.9 提供安全输入；

j) 7.10 指定安全要求；

k) 7.11 验证和证实安全性。

9.1.5 项目实施要求

安全项目过程中5个要求项的过程完整、明确，应基本达到每个要求项的目标；组织内的个人可识别出一个行动应被执行，并同意这个行动会在需要时执行。

a) 8.2 质量保证；

b) 8.3 管理配置；

c) 8.4 管理项目风险；

d) 8.5 监控技术活动；

e) 8.6 计划技术活动。

9.2 第二级

9.2.1 工程目标和范围

目标：在这一级别，资格保障要求满足，组织保障、工程实施和项目实施的基本要求项是经过计划并被跟踪。

范围：应验证特定步骤的执行工作产品应符合指定的标准和需求；测量用于跟踪要求项的执行情况；组织能够基于实际执行活动进行管理；本级别除去对基本要求项的要求外，还对要求项中的关键要求子项进行了特别要求；安全工程除满足第一级的要求外，还应保证计算机信息系统达到GA/T 391—2002中6.2、GA/T 390—2002中5.2的要求。

9.2.2 资格保障要求

满足下列关键资格要求子项的目标：

a) 5.1 国家主管部门认可四级集成资质；

b) 5.2 国家主管部门认可服务人员资质；

c) 5.3.5 国家主管部门认可五级服务单位资质；
d) 5.4.1 国家主管部门认可信息安全产品许可证书；
e) 5.4.2 操作系统符合保护等级操作系统同级要求；
f) 5.6.1 符合保护等级密码管理指南同级别要求；
g) 5.6.2 密码产品为国家批准的密码产品；
h) 5.6.3 来源于为国家批准的定点销售单位产品；
i) 5.6.4 研制来源于国家批准的密码研制单位；
j) 5.7 系统符合公共安全的相关法律、法规。

9.2.3 组织保障要求

组织保障基本要求项是经计划并被跟踪。应验证特定步骤的执行；工作产品应符合指定的标准和需求；测量用于跟踪要求项的执行情况；组织能够基于实际执行活动进行管理；本级别除去对组织保障要求中 6 个要求项的过程完整、明确，除完全达到每个要求项的要求外，还对以下要求项中的关键要求子项进行了特别要求。

a) 6.1 定义组织的系统工程过程；
b) 6.1.4 定义剪裁指南；
c) 6.2.2 评定过程；
d) 6.4.8 监视系统工程支持环境；
e) 6.5.1 确定培训要求；
f) 6.5.6 评估培训的有效性；
g) 6.5.8 维护培训材料；
h) 6.6.1 确定系统的组件或服务；
i) 6.6.3 选择供应商或销售商；
j) 6.6.4 提供期望。

9.2.4 工程实施要求

工程实施基本要求项经计划并被跟踪。应验证特定步骤的执行；工作产品应符合指定的标准和需求；测量用于跟踪要求项的执行情况；工程实施能够基于实际执行活动进行管理。本级别除去对安全工程实施中 11 个要求项过程完整、明确，除完全达到每个要求项的要求外，还对以下要求项中的关键要求子项进行了特别要求。

a) 7.1.5 管理安全服务及控制机制；
b) 7.2.7 监视影响；
c) 7.3.7 监视风险及其特征；
d) 7.4.7 监视威胁及其特征；
e) 7.5.6 监视脆弱性及其特征；
f) 7.6.4 控制保证证据；
g) 7.6.6 提供保证论据；
h) 7.8.2 分析事件记录；
i) 7.8.3 监视变化；
j) 7.8.4 识别安全突发事件；
k) 7.8.5 监视安全防护措施；
l) 7.8.6 检查安全态势；
m) 7.8.7 管理安全突发事件响应；
n) 7.8.8 保护安全监视的记录数据；
o) 7.9.4 识别安全选项；

p) 7.10.3 识别可用的法律、策略和约束；
q) 7.10.7 定义安全相关需求；
r) 7.11.2 确定验证和证实的目标；
s) 7.11.3 定义验证和证实方法；
t) 7.11.4 执行验证；
u) 7.11.5 执行证实；
v) 7.11.6 提供验证和证实的结果。

9.2.5 项目实施要求

项目实施基本要求项是经计划并被跟踪的。应验证特定步骤的执行；工作产品应符合指定的标准和需求；测量用于跟踪要求项的执行情况；项目实施能够基于实际执行活动进行管理。本级别除去对安全项目实施中5个要求项过程完整、明确，除完全达到每个要求项的要求外，还对以下要求项中的关键要求子项进行了特别要求。

a) 8.2.2 监视所定义过程的一致性；
b) 8.2.3 测量工作产品的质量；
c) 8.2.4 测量过程质量；
d) 8.2.5 分析质量测量；
e) 8.2.8 检测修正行为要求；
f) 8.4.3 标识风险；
g) 8.4.4 评估风险；
h) 8.4.5 复查风险评估；
i) 8.4.6 执行风险降低活动；
j) 8.4.7 跟踪风险降低活动；
k) 8.5.3 跟踪项目资源；
l) 8.5.4 跟踪技术参数；
m) 8.5.5 复查项目执行；
n) 8.5.7 采取修正行动；
o) 8.6.9 设立技术参数；
p) 8.6.11 复查并认可工程计划。

9.3 第三级

9.3.1 工程目标和范围

目标：在这一级别，要求满足资格保障要求；组织保障、工程实施和项目实施按照充分定义的过程执行(充分定义的过程是依据对文档化的标准过程进行裁剪并经批准的过程)；本级别利用组织范围内的过程标准来管理和规划，在实现第二级工程管理目标的基础上，要求对用户、系统资源和工程过程进行规范记录，对要求和文档清单建立健全的一系列安全管理制度，实现制度化管理。

范围：通过管理活动保证计算机信息系统达到GA/T 390—2002中6.3、GA/T 391—2002中5.3的要求。

9.3.2 资格保障要求

满足以下资格清单要求子项的目标：

a) 5.1.3 国家主管部门认可三级集成资质；
b) 5.2 国家主管部门认可服务人员资质；
c) 5.3.4 国家主管部门认可四级服务单位资质；
d) 5.4.1 国家主管部门认可信息安全产品许可证书；
e) 5.4.2 操作系统符合保护等级操作系统同级要求；

f) 5.5.1 监理公司具有信息安全监理资质证书；

g) 5.6.1 符合保护等级密码管理指南同级别要求；

h) 5.6.2 密码产品为国家批准的密码产品；

i) 5.6.3 来源于国家批准的定点销售单位产品；

j) 5.6.4 研制来源于为国家批准的密码研制单位；

k) 5.7 系统符合公共安全的相关法律、法规。

9.3.3 组织保障要求

在这一级别，组织保障按照充分定义的过程执行，充分定义的过程是依据对文档化的标准过程进行裁剪并经批准的过程版本；本级别利用组织范围内的过程标准来管理和规划，在实现第二级工程管理目标的基础上，要求实现制度化管理。

除满足二级组织保障要求项外还应满足以下关键要求子项的目标并规范化、制度化管理：

a) 6.1.2 收集过程资产；

b) 6.1.3 开发组织的系统工程过程；

c) 6.2.5 沟通过程改进；

d) 6.3.5 确保关键组件的可用性；

e) 6.3.6 插入产品技术；

f) 6.4.2 维持技术认识；

g) 6.4.3 确定支持需求；

h) 6.5.3 确保技能和知识的可用性；

i) 6.5.4 准备培训材料；

j) 6.5.5 培训人员；

k) 6.5.7 维护培训记录；

l) 6.6.2 确定胜任的供应商或销售商；

m) 6.6.5 维持沟通。

9.3.4 工程实施要求

在这一级别，工程实施按照充分定义的过程执行，充分定义的过程是依据对文档化的标准过程进行裁剪并经批准的过程；利用组织范围内的过程标准来管理和规划，在达到第二级工程管理目标的基础上，要求对用户、系统资源和工程过程进行规范记录，建立健全一系列的安全管理制度，实现制度化管理。除满足二级所有要求项和关键要求子项外，还应满足以下关键子项的要求并实现规范化、制度化管理：

a) 7.1.2 建立安全职责；

b) 7.1.3 管理安全配置；

c) 7.1.4 管理安全意识、培训和教育大纲；

d) 7.2.2 对影响进行优先级排列；

e) 7.2.3 识别系统资产；

f) 7.2.4 选择影响的度量；

g) 7.2.5 标识度量关系；

h) 7.2.6 识别和特征化影响；

i) 7.3.2 识别风险；

j) 7.3.3 评估风险；

k) 7.3.4 评估总体不确定性；

l) 7.4.2 识别自然威胁；

m) 7.4.3 识别人为威胁；

n) 7.4.4 识别威胁的测量尺度；
o) 7.4.5 评估威胁影响的效果；
p) 7.4.6 评估威胁的可能性；
q) 7.5.3 识别脆弱性；
r) 7.5.4 收集脆弱性数据；
s) 7.7.4 促进协调；
t) 7.9.5 分析工程选项的安全性；
u) 7.9.6 提供安全工程指南；
v) 7.10.4 识别系统安全关联性。

9.3.5 项目实施要求

在这一级别，项目实施按照充分定义的过程执行，充分定义的过程是依据对文档化的标准过程进行裁剪并经批准的过程；本级别利用组织范围内的过程标准来管理和规划，在实现第二级项目管理目标的基础上，要求对用户、系统资源和工程过程进行规范记录，建立健全一系列的安全管理制度，实现制度化管理。除满足二级所有要求项外，还应满足以下关键要求子项的要求并规范化、制度化管理：

a) 8.2.7 发起改进质量的活动；
b) 8.3.3 确定配置单元；
c) 8.3.5 控制变化；
d) 8.3.6 沟通配置状况；
e) 8.5.6 分析项目问题；
f) 8.6.2 识别关键资源；
g) 8.6.3 估计项目范围；
h) 8.6.8 开发项目进度表；
i) 8.6.10 开发技术管理计划。

9.4 第四级

9.4.1 工程目标和范围

目标：在达到第三级管理目标的基础上，要求计算机信息系统的使用单位，将安全工程过程、安全项目过程和组织保障过程的有效性，程序化、周期化，能够使用有效的控制手段对要求和文档清单进行过程管理。

范围：通过工程活动保证计算机信息系统达到 GA/T 390—2002 中 6.4、GA/T 391—2002 中 5.4 的要求。

9.4.2 资格保障要求

满足以下关键要求子项的资格目标要求：

a) 5.1.2 国家主管部门认可二级集成资质；
b) 5.2 国家主管部门认可服务人员资质；
c) 5.3.3 国家主管部门认可三级服务单位资质；
d) 5.4.1 国家主管部门认可信息安全产品许可证书；
e) 5.4.2 操作系统符合保护等级操作系统同级要求；
f) 5.5.1 监理公司具有信息安全监理资质证书；
g) 5.6.1 符合保护等级密码管理指南同级别要求；
h) 5.6.2 密码产品为国家批准的密码产品；
i) 5.6.3 来源于为国家批准的定点销售单位产品；
j) 5.6.4 研制来源于为国家批准的密码研制单位；
k) 5.7 系统符合公共安全的相关法律、法规。

9.4.3 组织保障要求

组织保障要求项中6个过程完整，在文档清单要求中除了满足第三级要求外，还应满足以下文档清单的要求，且所有文档清单的描述应完整、全面，文档化管理应能够与日常运行和历史资料进行对比，能够使用有效的控制手段对要求和文档清单进行过程管理。

a) 6.1.1 制定过程目标；

b) 6.2.4 改变标准过程；

c) 6.4.4 获得系统工程支持环境；

d) 6.4.7 维护环境；

e) 6.5.2 选择知识或技能的获取模式。

9.4.4 工程实施要求

安全工程中11个要求项的过程完整、明确，完全达到每个要求项的目标、概述要求，所有要求子项提供的证据材料应完整、全面，文档化管理应能够与日常运行和历史资料进行对比，能使用有效的控制手段对要求和关键要求子项进行过程管理。

9.4.5 项目实施要求

项目过程中5个要求项的过程完整、明确，除完全达到每个要求项的所有要求外，所有要求子项提供的证据材料应完整、全面，文档化管理应能够与日常运行和历史资料进行对比，能使用有效的控制手段对要求和关键要求子项进行过程管理。

9.5 第五级

9.5.1 工程目标和范围

目标：在这一级别应基于组织的目标针对过程有效性和效率建立量化执行指标，通过已定义过程和新概念、新技术的量化反馈来保证对实现这些目标的过程进行连续改进。

范围：在这一级别，除满足第四级的要求外，组织的全面安全计划应成为组织文化的有机组成部分，保证具有持续完善的工程过程管理、项目过程管理和组织保障管理，并对计算机信息系统安全实施全面的质量管理，能够利用历史资料和使用模型对工程进行优化；通过管理活动保证计算机信息系统达到GA/T 390—2002中6.5、GA/T 391—2002中5.5的要求。

9.5.2 资格保障要求

满足以下关键资格保障要求子项的目标：

a) 5.1.1 国家主管部门认可一级集成资质；

b) 5.2 国家主管部门认可服务人员资质；

c) 5.3.2 国家主管部门认可二级服务单位资质；

d) 5.4.1 国家主管部门认可信息安全产品许可证书；

e) 5.4.2 操作系统符合保护等级操作系统同级要求；

f) 5.5.1 监理公司具有信息安全监理资质证书；

g) 5.6.1 符合保护等级密码管理指南同级别要求；

h) 5.6.2 密码产品为国家批准的密码产品；

i) 5.6.3 来源于为国家批准的定点销售单位产品；

j) 5.6.4 研制来源于为国家批准的密码研制单位；

k) 5.7 系统符合公共安全的相关法律、法令、法规。

9.5.3 组织保障要求

在这个级别上，应基于组织的目标针对过程有效性和效率建立量化执行目标；通过执行已定义过程新概念、新技术的量化反馈来保证对实现这些目标的过程进行连续改进；除满足第四级的要求外，还应要求组织的全面安全计划成为组织文化的有机组成部分；保证具有持续完善的组织保障管理，并对计算机信息系统安全实施全面的质量管理；安全组织保障过程中6个要求项的过程应完整、明确，除完全达

到每个要求项的所有要求外，所有要求项中的要求子项应完整并满足要求，也就是在满足第四级的组织保障基础上，还应满足以下关键要求子项的要求并且能与历史资料进行对比，利用模型进行优化：

a) 6.2.3 规划过程改进；
b) 6.3.2 定义产品进化；
c) 6.3.3 标识新生产技术；
d) 6.3.4 适应开发过程；
e) 6.4.5 剪裁系统工程支持环境；
f) 6.4.6 插入新技术。

9.5.4 工程实施要求

在这个级别上，应基于组织的目标针对过程有效性和效率建立量化执行目标；通过执行已定义过程和新概念、新技术的量化反馈来保证对实现这些目标的过程进行连续改进；除满足第四级的要求外，要求组织的全面安全计划应成为组织文化的有机组成部分；保证具有持续完善的工程实施管理，并对计算机信息系统安全实施全面的质量管理；工程实施要求中 11 个要求项的过程应完整、明确，要完全达到每个要求项的所有要求，所有要求项中的要求子项也应完整并满足要求，要求项和要求子项能够根据组织的特点进行添加与升级，并且能与历史资料进行对比，利用模型进行优化。

9.5.5 项目实施要求

在这个级别上，应基于组织的应用目标针对过程有效性和效率建立量化执行目标；通过执行已定义过程和有创建的新概念、新技术的量化反馈来保证对这些目标进行连续过程改进；除满足第四级的要求外，要求组织的全面安全计划成为组织文化的有机组成部分；保证具有持续完善的项目过程管理，并对计算机信息系统安全实施全面的质量管理保证体系；项目实施要求中 5 个要求项的过程应完整、明确，除完全达到每个要求项的所有要求外，所有要求项中的要求子项应完整并满足要求；要求项和要求子项能够根据组织的特点进行添加与升级，以及能与历史资料进行对比，利用模型对资料进行优化。

9.6 安全保护等级划分安全功能要求对照表

按《计算机信息系统安全保护等级划分准则》所描述的每一个安全保护级对安全工程的不同要求，可以得到每个安全保护级的资格保障要求、组织保障要求、工程实施要求、项目实施要求的表，详见附录 A 的表一。

附　录　A
（资料性附录）
等级要求对照表

表 A.1　安全保护等级划分安全功能要求表

安　全　要　求	安全保护等级				
	第一级	第二级	第三级	第四级	第五级
资格保障要求					
5.1—信息系统集成资质要求					
5.1.1—国家主管部门认可一级集成资质		√			
5.1.2—国家主管部门认可二级集成资质			√		
5.1.3—国家主管部门认可三级集成资质				√	
5.1.4—国家主管部门认可四级集成资质					√
5.2—信息安全人员资质要求					
国家主管部门认可安全服务人员资质		√	√	√	√
5.3　信息安全第三方服务要求					
5.3.1—国家主管部门认可一级服务单位资质					
5.3.2—国家主管部门认可二级服务单位资质					√
5.3.3—国家主管部门认可三级服务单位资质				√	
5.3.4—国家主管部门认可四级服务单位资质			√		
5.3.5—国家主管部门认可五级服务单位资质		√			
5.4—信息安全产品要求					
5.4.1　国家主管部门认可安全产品许可证书	√	√	√	√	√
5.4.2—操作系统符合等级操作系统同级要求	√	√	√	√	√
5.5—信息安全监理要求					
5.5.1—监理公司具有信息安全监理资质证书			√	√	√
5.6—密码管理要求					
5.6.1—符合保护等级密码指南同级别要求	√	√	√	√	√
5.6.2—密码产品为国家批准的密码产品	√	√	√	√	√
5.6.3—来源为国家批准的定点销售单位产品	√	√	√	√	√
5.6.4—来源于为国家批准的密码研制单位	√	√	√	√	√
5.7　其他要求					
系统符合公共安全的相关法律、法规	√	√	√	√	√
组织保障要求					
6.1—定义组织的系统工程过程	√	√	√	√	√
6.1.1—制定过程目标				√	√
6.1.2—收集过程资产			√	√	√
6.1.3　开发组织的系统工程过程			√	√	√
6.1.4—定义剪裁指南		√	√	√	√
6.2—改进组织的系统工程过程	√	√	√	√	√

表 A.1（续）

安　全　要　求	安全保护等级				
	第一级	第二级	第三级	第四级	第五级
6.2.2—评定过程		√	√	√	√
6.2.3—规划过程改进					√
6.2.4—改变标准过程				√	√
6.2.5—沟通过程改进			√	√	√
6.3—管理系列产品进化	√	√	√	√	√
6.3.2—定义产品进化					√
6.3.3—标识新生产技术					√
6.3.4—适应开发过程					√
6.3.5—确保关键组件的可用性			√	√	√
6.3.6—插入产品技术			√	√	√
6.4—管理系统工程支持环境	√	√	√	√	√
6.4.2—维持技术认识			√	√	√
6.4.3—确定支持需求			√	√	√
6.4.4—获得系统工程支持环境				√	√
6.4.5—剪裁系统工程支持环境					√
6.4.6—插入新技术					√
6.4.7—维护环境				√	√
6.4.8—监视系统工程支持环境		√	√	√	√
6.5—培训	√	√	√	√	√
6.5.1—确定培训要求		√	√	√	√
6.5.2—选择知识或技能的获取模式				√	√
6.5.3—确保技能和知识的可用性			√	√	√
6.5.4—准备培训材料			√	√	√
6.5.5—培训人员			√	√	√
6.5.6—评估培训的有效性		√	√	√	√
6.5.7—维护培训记录			√	√	√
6.5.8—维护培训材料		√	√	√	√
6.6—与供应商协调	√	√	√	√	√
6.6.1—确定系统的组件或服务		√	√	√	√
6.6.2—确定胜任的供应商或销售商			√	√	√
6.6.3—选择供应商或销售商		√	√	√	√
6.6.4—提供期望		√	√	√	√
6.6.5—维持沟通			√	√	√
工程实施要求					
7.1—管理安全控制				√	√
7.1.2—建立安全职责	√	√	√	√	√
7.1.3—管理安全配置			√	√	√
7.1.4—管理安全意识、培训和教育			√	√	√
7.1.5—管理安全服务及控制机制			√	√	√

表 A.1（续）

安全要求	安全保护等级				
	第一级	第二级	第三级	第四级	第五级
7.2—评估影响		√	√	√	√
7.2.2—对影响进行优先级排列	√	√	√	√	√
7.2.3—识别系统资产			√	√	√
7.2.4—选择影响的度量			√	√	√
7.2.5—标识度量关系			√	√	√
7.2.6—识别和特征化影响			√	√	√
7.2.7—监视影响			√	√	√
7.3—评估安全风险		√	√	√	√
7.3.2—选择风险分析方法	√	√	√	√	√
7.3.3—识别风险				√	√
7.3.4—评估风险			√	√	√
7.3.5—评估总体不确定性			√	√	√
7.3.6—风险优先级排列				√	√
7.3.7—监视风险及其特征		√	√	√	√
7.4—评估威胁	√	√	√	√	√
7.4.2—识别自然威胁			√	√	√
7.4.3—识别人为威胁			√	√	√
7.4.4—识别威胁的测量尺度			√	√	√
7.4.5—评估威胁影响的效果			√	√	√
7.4.6—评估威胁的可能性			√	√	√
7.4.7—监视威胁及其特征		√	√	√	√
7.5—评估脆弱性	√	√	√	√	√
7.5.2—选择脆弱性分析方法				√	√
7.5.3—识别脆弱性			√	√	√
7.5.4—收集脆弱性数据			√	√	√
7.5.5—综合系统脆弱性				√	√
7.5.6—监视脆弱性及其特征		√	√	√	√
7.6—建立保证论据	√	√	√	√	√
7.6.2—识别保证目标				√	√
7.6.3—定义保证策略		√	√	√	√
7.6.4—控制保证证据				√	√
7.6.5—分析证据		√	√	√	√
7.6.6—提供保证论据	√	√	√	√	√
7.7—协调安全				√	√
7.7.2—定义协调目标				√	√
7.7.3—识别协调机制			√	√	√
7.7.4—促进协调				√	√
7.7.5—协调安全决定和建议	√	√	√	√	√
7.8—监视安全态势		√	√	√	√

表 A.1（续）

安　全　要　求	安全保护等级				
	第一级	第二级	第三级	第四级	第五级
7.8.2—分析事件记录		√	√	√	√
7.8.3—监视变化		√	√	√	√
7.8.4—识别安全突发事件		√	√	√	√
7.8.5—监视安全防护措施		√	√	√	√
7.8.6—检查安全态势		√	√	√	√
7.8.7—管理安全突发事件响应		√	√	√	√
7.8.8—保护安全监视的记录数据	√	√	√	√	√
7.9—提供安全输入				√	√
7.9.2—理解安全输入要求				√	√
7.9.3—确定安全约束和考虑		√	√	√	√
7.9.4—识别安全选项			√	√	√
7.9.5—分析工程选项的安全性			√	√	√
7.9.6—提供安全工程指南				√	√
7.9.7—提供运行安全指南	√	√	√	√	√
7.10—指定安全要求				√	√
7.10.2—获得对安全要求的理解		√	√	√	√
7.10.3—识别可用法律、策略和约束			√	√	√
7.10.4—识别系统安全关联性				√	√
7.10.5—获取系统运行的安全思想				√	√
7.10.6—获取安全的高层目标		√	√	√	√
7.10.7—定义安全相关需求				√	√
7.10.8—达成安全协议	√	√	√	√	√
7.11—验证和证实安全性		√	√	√	√
7.11.2—确定验证和证实的目标		√	√	√	√
7.11.3—定义验证和证实方法		√	√	√	√
7.11.4—执行验证		√	√	√	√
7.11.5—执行证实		√	√	√	
7.11.6—提供验证和证实的结果					√
项目实施要求					
8.2—质量保证	√	√	√	√	√
8.2.2　监视所定义过程的一致性		√	√	√	√
8.2.3　测量工作产品的质量		√	√	√	√
8.2.4—测量过程质量		√	√	√	√
8.2.5—分析质量测量		√	√	√	√
8.2.6—参与				√	√
8.2.7—发起改进质量的活动			√	√	√
8.2.8—检测修正行为要求		√	√	√	√
8.3—管理配置	√	√	√	√	√
8.3.2—建立配置管理方法				√	√

表 A.1（续）

安　全　要　求	安全保护等级				
	第一级	第二级	第三级	第四级	第五级
8.3.3—确定配置单元			√	√	√
8.3.4—维护工作产品基线				√	√
8.3.5—控制变化			√	√	√
8.3.6—沟通配置状况			√	√	√
8.4—管理项目风险	√	√	√	√	√
8.4.2—开发风险管理方法				√	√
8.4.3—标识风险		√	√	√	√
8.4.4—评估风险		√	√	√	√
8.4.5—复查风险评估		√	√	√	√
8.4.6—执行风险降低活动		√	√	√	√
8.4.7—跟踪风险降低活动		√	√	√	√
8.5—监控技术活动	√	√	√	√	√
8.5.2—指导技术活动				√	√
8.5.3—跟踪项目资源		√	√	√	√
8.5.4—跟踪技术参数		√	√	√	√
8.5.5—复查项目执行		√	√	√	√
8.5.6—分析项目问题			√	√	√
8.5.7—采取修正行动		√	√	√	√
8.6—计划技术活动	√	√	√	√	√
8.6.2—识别关键资源			√	√	√
8.6.3—估计项目范围			√	√	√
8.6.4—估算项目费用				√	√
8.6.5—确定工程过程				√	√
8.6.6—确定技术活动				√	√
8.6.7—定义项目界面				√	√
8.6.8—开发项目进度表			√	√	√
8.6.9—设立技术参数		√	√	√	√
8.6.10—开发技术管理计划			√	√	√
8.6.11—复查并认可工程计划		√	√	√	√

注：其中，“√”号表示具有该要求。

参 考 文 献

[1] TCSEC 可信计算机系统评估准则—1983
[2] ITSEC 信息技术安全评定标准—1991
[3] CTCPEC 可信计算机产品评价准则—1993
[4] FC 联邦准则—1993
[5] GB/T 18336—2001 信息技术 安全技术 信息技术安全性评估准则(等同于 ISO/IEC 15408:2000)
[6] ISO/IEC 17799:2000 信息技术 信息安全管理实施细则
[7] GB/T 9387.2—1995 信息处理系统 开放系统互连 基本参考模型 第 2 部分:安全体系结构(ISO/IEC 7498-2:1989)
[8] ISO 9000:2000
[9] ISO 9001:2000
[10] SSE-CMM 系统安全工程能力成熟度模型 V2.0 2002